IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLNOIS
EASTERN DIVISION

BENNIE ARCHEY,	)	Case No.: 1:20-cv-05247
Plaintiff,	)	
v.	)	Honorable Franklin U. Valderrama
OSMOSE UTILITIES SERVICES, INC.,	)	
Defendant.	)	Magistrate Judge M. David Weisman

PLAINTIFF'S RESPONSE TO DEFENDANT'S MOTION TO DISMISS COUNTS II AND COUNTS III WITHOUT LEAVE TO AMEND

NOW COMES Plaintiff, BENNIE ARCHEY ("Archey"), by and through his attorneys, Pietrucha Law Firm LLC and Custardo Law LLC, for his Response to the Defendant's Motion to Dismiss ("Motion"), and in support, states as follows:

LEGAL STANDARD

When ruling on a motion to dismiss under Federal Rule of Civil Procedure Rule 12(b)(6), the court must consider all the alleged facts in the complaint as true, draw all reasonable inferences in plaintiff's favor, and ask "whether there is any possible interpretation of the complaint under which it can state a claim." *Flannery v. Recording Indus. Ass'n of Am.,* 354 F.3d 632, 640 (7th Cir. 2004). A complaint need not contain "[d]etailed factual allegations," but "must contain sufficient factual matter, accepted as true, to 'state a claim to relief that is plausible on its face.'" *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007)). A claim must stand when its factual content allows the court to draw a reasonable inference that the defendants are liable for the misconduct alleged. *Id.* Under Federal Rule of Civil Procedure Rule 8(a)(2), a Complaint must include "a short and plain statement of the claim showing that the pleader is entitled to relief." Fed. R. Civ. P. 8(a)(2). Under federal notice-pleading standards, a plaintiff's "[f]actual allegations must be enough to raise a right to relief above the speculative level." *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 555 (2007).

By the same token, "the Supreme Court has signaled on several occasions that it has not amended the rules of civil procedure *sub silentio* to abolish notice pleading and return to the old fact

pleading standards that pre-dated the modern civil rules." *Alexander v. United States,* 721 F.3d 418, 422 (7th Cir. 2013). Thus, a plaintiff is not required to include "detailed factual allegations" to survive a motion to dismiss. *Id.* Nor is "plausibility" the same as "probability," and it is therefore inappropriate for the Court to "stack up inferences side by side and allow the case to go forward only if the plaintiff s inferences seem more compelling than the opposing inferences." *Id.* (citation omitted). Instead, "the plausibility requirement demands only that a plaintiff provide sufficient detail to present a story that holds together." *Id.* (internal quotation marks and citation omitted). Therefore, a claim "has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Id.* (citing *Twombly*, 550 U.S.at 556). A plaintiff must plead enough details "to present a story that holds together…[b]ut the proper question to ask is still 'could these things have happened,' not 'did they happen.'" *Carlson v. CSX Transp., Inc.,* 758 F.3d 819, 827 (7th Cir. 2014) (quoting *Swanson v. Citibank, N.A.,* 614 F.3d 400, 404-05 (7th Cir. 2010)) (citations omitted), and the Court will accept Plaintiff's claims "as true all of the well pleaded facts in the complaint and draw all reasonable inferences in favor of the plaintiff." Platt v. Brown, 872 F.3d 848, 851 (7th Cir. 2017).

ARGUMENT

Plaintiff alleges more than sufficient facts, not mere legal conclusions, to support a bona fide claim of breach of implied contract in employment (Count II) and a claim for violation of the Illinois Consumer Fraud and Deceptive Business Practices Act (Count III).

I. COUNT II STATES A CLAIM FOR BREACH OF IMPLIED CONTRACT.

In Illinois, the elements of an implied contract "substantially overlap" with those of an express contract. *Landale Signs & Neon, Ltd. v. Runnion Equip. Co.,* 274 F. Supp. 3d 787, 792 (N.D. Ill. 2017); *New v. Verizon Commc'ns, Inc.,* 635 F. Supp. 2d 773, 782-83 (N.D. Ill. 2008) ("In Illinois, in order to prove an implied contract, the party asserting the contract must show the same elements as an express

contract, as well as a meeting of the minds and a mutual intent to contract."). An implied in fact contract is created by the parties' conduct and contains all the elements of an express contract — offer, acceptance, and consideration — as well as a meeting of the minds. *Brody v. Finch Univ. of Health Scis./Chi. Medical Sch.*, 698 N.E.2d 257, 265 (1998).

This Court analyzed a very similar issue to the case at bar in *In re Michaels Stores Pin Pad Litigation*. In May 2011, specialty arts and crafts retailer Michaels Stores, Inc. reported that the PIN pad terminals, used to process credit and debit card payments, may have been tampered with in its Chicago area stores. *In re Michaels Stores Pin Pad Litigation*, 830 F. Supp. 2d 518, 522 (N.D.Ill. November 23, 2011). Michaels later revealed that between February 8, 2011, and May 6, 2011, skimmers placed approximately ninety tampered PIN pads in eighty Michaels stores across twenty states. *Id.* A class action lawsuit on behalf of all consumers whose financial information was stolen from Michaels followed. *Id.* Plaintiffs alleged that Michaels failed to adequately protect their financial information and failed to promptly and properly notify consumers of the security breach. *Id.* Plaintiffs further alleged that the data breach resulted in unauthorized withdrawals from their bank accounts and/or bank fees. *Id.* Plaintiffs asserted claims under the Illinois Consumer Fraud and Deceptive Business Practices Act, 815 Ill. Comp. Stat. 505/1, *et seq*., as well as a breach of implied contract, amongst other causes of action, and Michaels brought a 12(b)(6) motion to dismiss. *Id.*

This Court in *In re Michaels Stores Pin Pad Litigation* denied defendant Michaels' 12(b)(6) motion to dismiss, holding that the allegations demonstrated the existence of an implicit contractual relationship between Plaintiffs and Michaels, which obligated Michaels to take reasonable measures to protect Plaintiffs' financial information and notify Plaintiffs of a security breach within a reasonable amount of time. *Id.*, at 522 (citing *Anderson v. Hannaford Bros.*, 659 F.3d 151, 153-54 (1st Cir.2011) ("[w]hen a customer uses a credit card in a commercial transaction, she intends to provide the data to the merchant only […] and does not expect — and certainly does not intend — the merchant to allow

unauthorized third parties to access that data. […] A jury could reasonably conclude, therefore, that an implicit agreement to safeguard the data is necessary to effectuate the contract.")

Here, like in *In re Michaels Stores Pin Pad Litigation*, ARCHEY alleges that after the July 13, 2020, cyberattack on OSMOSE, OSMOSE launched an investigation and determined that "one or more files containing ARCHEY's personal information were accessed by at least one unauthorized third party." Am. Compl., ¶¶ 29-30. As ARCHEY was required to provide OSMOSE his personal information as a condition of employment (Am. Compl., ¶ 38), he expected OSMOSE to take reasonable steps to secure and safeguard his personal information and likewise to take reasonable steps in the event of unauthorized disclosures of such information. When sharing this personal information, ARCHEY did not expect OSMOSE would allow unauthorized third parties to access that data. In fact, ARCHEY would not have provided and entrusted his personal information to OSMOSE in order to be employed by OSMOSE, or would have sought additional compensation, if OSMOSE had revealed it was not reasonably safeguarding or otherwise reasonably notifying ARCHEY of unauthorized disclosures. Am. Compl., ¶ 41. Thus, a jury could reasonably conclude, therefore, that an implied agreement to safeguard the data was necessary to effectuate the implied contract.

The cases cited by OSMOSE in its Motion, can be easily distinguished from the case at hand. Particularly, OSMOSE cites *Dinerstein v. Google, LLC*, No. 19 C 4311, 2020 WL 5296920, at *21 (N.D. Ill. Sept. 4, 2020) a case in which the Court dismissed a claim for breach of implied contract for failure to adequately plead damages because "[i]n Illinois, the elements of an implied contract substantially overlap with those of an express contract." (See ECF No. 25, p. 5.). Dissimilarly, in the employment relationship between ARCHEY and OSMOSE, it appears there was no express contract between ARCHEY and OSMOSE related to data security; thus, only an implied contract would apply to this case. Even though the Court dismissed the breach of implied contract claim in *Dinerstein*, it was

because there was an express contract between the parties. Even then, *Dinerstein* states that damages are not necessarily a requirement of a breach of contract action. *See Dinerstein*, 2020 WL 5296920, at *9 ("Where a right of action for breach exists, but no harm was caused by the breach, […] judgment will be given for nominal damages, a small sum fixed without regard to the amount of harm.").

This Court in *Dinerstein* also cited to out-of-circuit case law in support. *See Springer v. Cleveland Clinic Emp. Health Plan Total Care,* 900 F.3d 284, 287 (6th Cir. 2018) (citations omitted) ("Like any private contract claim, his injury does not depend on allegation of financial loss. His injury is that he was denied the benefit of his bargain. […] The injury therefore stemmed from traditional principles of contract law that did not depend on financial harm."); *Kuhns v. Scottrade, Inc.*, 868 F.3d 711, 716 (8th Cir. 2017) (quoting *Carlsen v. GameStop, Inc.,* 833 F.3d 903, 909 (8th Cir. 2016)) ("[A] party to a breached contract has a judicially cognizable interest for standing purposes, regardless of the merits of the breach alleged."); *In re Facebook Internet Tracking Litig.,* 263 F. Supp. 3d 836, 844 (N.D.Cal.2017) ("Actual damages are not required to establish standing for contractual claims."), 956 F.3d 589 (9th Cir. 2020).

Here, ARCHEY has an expectation of privacy for his personal data and OSMOSE breached that duty when hackers accessed OSMOSE's employees' data. ARCHEY was denied the benefit of the bargain and he must be allowed to pursue his breach of implied contract claim at this stage of the pleadings. Accordingly, Defendant OSMOSE' Motion to Dismiss Plaintiff ARCHEY's Count II without leave to amend must be denied, and the Court should also reserve Plaintiff's right to request leave to amend as investigation into the relevant data breach continues.

A. ARCHEY Sufficiently Pleads Mutual Assent and Breach of an Implied Contract for Data Security.

In its Motion, OSMOSE incorrectly argues that "[b]are allegations that Plaintiff provided his personal information to his employer do not sufficiently state mutual assent to create an implied contractual obligation on Osmose's part to protect that information in some undefined way." (See

ECF No. 25, p. 11) It is worth noting again that under federal pleading standards, Plaintiff does not have to include "detailed factual allegations" to survive dismissal. *Alexander*, 721 F.3d at 422. Because notice pleading standards apply, the question is whether Plaintiff has alleged enough detail to "present a story that holds together." *Id.* (citation omitted).

As ARCHEY states in his Complaint, OSMOSE was required, pursuant to Illinois Personal Information Protection Act, 815 ILCS 530/1 *et seq.* ("IPIPA"), to implement and maintain reasonable security measures to protect ARCHEY's personal information, and to notify him regarding any unauthorized disclosure in the most expedient time possible and without unreasonable delay. Am. Compl., ¶ 45. Beyond the Illinois statute which requires an employer to protect its employees' data, there is a scarcity of case law in the Seventh Circuit on the issue. However, courts in other Circuits have found that employers are required to protect their employees' data. In *Sackin v. Transperfect Glob. Inc.,* the Southern District of New York held that employers have a duty to take reasonable precautions to protect the information that they require from employees; and thus, have a duty to protect their employees' personal information from data breaches. No. 17 Civ. 1469, 2017 U.S. Dist. LEXIS 164933 (S.D.N.Y. Oct. 4, 2017). The Court reasoned that the employer is in the best position to avoid the harm to employees, and that potential liability to employers provides an economic incentive to act reasonably in protecting employee data from the threat of cyberattack. *Id.*

Thus, just by entering into an employment relationship, there was mutual agreement between ARCHEY and OSMOSE to follow the law regarding the protection of employees' data. By OSMOSE failing to safeguard its' employees' personal information, and subsequently failing to timely notify ARCHEY that such personal information had been compromised, in violation of the IPIPA (*see* Am. Compl., ¶ 46), OSMOSE breached the implied contract. Accordingly, Defendant OSMOSE' Motion to Dismiss Plaintiff ARCHEY's Count II without leave to amend must be denied.

B. A Motion for Summary Judgment Would Fail.

The Seventh Circuit has held that documents referenced in the complaint and central to the claims asserted may be considered at the motion to dismiss stage without converting underlying motion to one for summary judgment. *Adams v. City of Indianapolis,* 742 F.3d 720, 729 (7th Cir. 2014). However, if, on a motion under Rule 12(b)(6), matters outside the pleadings are presented to and not excluded by the court, the motion must be treated as one for summary judgment under Rule 56. Fed. R. Civ. P. Rule 12(d). Under Rule 56, "a party may move for summary judgment, identifying each claim or defense — or the part of each claim or defense — on which summary judgment is sought." Fed. R. Civ. P. Rule 56(a). The court shall grant summary judgment if the movant shows that there is no genuine dispute as to any material fact and the movant is entitled to judgment as a matter of law. Fed. R. Civ. P. Rule 56(a).

Here, OSMOSE brings its Motion under 12(b)(6), yet offers a rather large amount of information outside of the pleadings. *See* ECF No. 25, *passim.* Therefore, if this Court converts OSMOSE's Motion to one for summary judgment, there are still too many genuine issues of material fact outstanding to grant OSMOSE judgment as a matter of law. Thus, OSMOSE's Motion to Dismiss Count II without leave to amend must be denied.

II. COUNT III STATES A CLAIM FOR VIOLATION OF THE ILLINOIS CONSUMER FRAUD AND DECEPTIVE BUSINESS PRACTICES ACT.

To state a claim under the Illinois Consumer Fraud Act ("ICFA"), a plaintiff must allege that (1) the defendant engaged in a deceptive or unfair practice, (2) the defendant intended for the plaintiff to rely on the deception, (3) the deception occurred in the course of conduct involving trade or commerce, (4) plaintiff sustained actual damages, and (5) such damages were proximately caused by the defendant's deception. *Martis v. Pekin Mem'l Hosp. Inc.*, 395 Ill.App.3d 943, 334 Ill.Dec. 772, 917 N.E.2d 598, 603 (2009). In its Motion, OSMOSE concedes on every element but actual damages. Thus, ARCHEY need only address his damages herein.

A. ARCHEY Suffered Actual Damages As A Result Of The Cyber Attack.

OSMOSE argues that ARCHEY fails to allege he suffered actual damage under the ICFA. *See* ECF No. 25, pp. 5-9. Only a person who suffers actual damage may bring an action under the ICFA. 815 Ill. Comp. Stat. 505/10a(a). The plaintiff must allege a purely economic injury, measurable by the plaintiff's loss. *Morris v. Harvey Cycle & Camper, Inc.,* 392 Ill.App.3d 399, 331 Ill. Dec. 819, 911 N.E.2d 1049, 1053 (2009); *see Mulligan v. QVC, Inc.*, 382 Ill.App.3d 620, 321 Ill.Dec. 257, 888 N.E.2d 1190, 1197-98 (2008) ("If the plaintiff is not materially harmed by the defendant's conduct, however flagrant it may have been, there may be no recovery.").

In *Remijas v. Neiman Marcus Group, LLC*, the Seventh Circuit addressed the issue of "damages" in a data breach case. Sometime in 2013, hackers attacked Neiman Marcus, a luxury department store, and stole the credit card numbers of its customers. *Remijas v. Neiman Marcus Group, LLC,* 794 F. 3d 688, 689 (7th Cir. 2015). In December 2013, the company learned that some of its customers had found fraudulent charges on their cards. *Id.*, at 689-90. On January 10, 2014, it announced to the public that the cyberattack had occurred and that between July 16, 2013, and October 30, 2013, approximately 350,000 cards had been exposed to the hackers' malware. *Id.*, at 690. In the wake of those disclosures, several customers brought a class action lawsuit seeking various forms of relief. *Id.* Defendant's motion to dismiss was granted and an appeal followed. *Id.* On appeal, the Seventh Circuit reversed and remanded. *Id.*

In *Neiman Marcus*, addressing the issue of "speculative damages", the Seventh Circuit held that "the risk that Plaintiffs' personal data will be misused by the hackers who breached Adobe's network is immediate and very real" because at "this stage in the litigation[1], it is plausible to infer that the

[1] The Seventh Circuit in *Neiman Marcus* also held that "fraudulent charges and identity theft can occur long after a data breach. [Plaintiff's Complaint] cites a Government Accountability Office Report that finds that 'stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years.' U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-07-737, REPORT TO CONGRESSIONAL REQUESTERS: PERSONAL INFORMATION 29 (2007). […] We

plaintiffs have shown a substantial risk of harm from the Neiman Marcus data breach. Why else would hackers break into a store's database and steal consumers' private information? Presumably, the purpose of the hack is, sooner or later, to make fraudulent charges or assume those consumers' identities." *Id.*, at 693. The Seventh Circuit held in *Neiman Marcus* that there was "no need to speculate as to whether [the Neiman Marcus customers'] information has been stolen and what information was taken," because Neiman Marcus admitted its data was breached. *Id.* The Seventh Circuit further held, "[r]equiring the plaintiffs to wait for the threatened harm to materialize in order to sue would create a different problem: the more time that passes between a data breach and an instance of identity theft, the more latitude a defendant has to argue that the identity theft is not 'fairly traceable' to the defendant's data breach." *Id.* (citing *In re Adobe Sys., Inc. Privacy Litig.,* 66 F.Supp.3d 1197, 1214 (N.D.Cal.2014)) (internal quotations omitted).

The Seventh Circuit in *Neiman Marcus* also made it a point to mention that:

> "Neiman Marcus offered one year of credit monitoring and identity-theft protection to all customers for whom it had contact information and who had shopped at their stores between January 2013 and January 2014. It is unlikely that it did so because the risk is so ephemeral that it can safely be disregarded. These credit-monitoring services come at a price that is more than *de minimis*. For instance, Experian offers credit monitoring for $4.95 a month for the first month, and then $19.95 per month thereafter. See http://www.experian.com/consumer-products/credit-monitoring.html. **That easily qualifies as a concrete injury**."

Neiman Marcus, 794 F. 3d at 694 (emphasis added).

Here, OSMOSE acknowledges that there was a "cyberattack [that] accessed systems containing folders with information related to current and former employees, including Plaintiff." See ECF No. 25, p. 1. "Osmose determined that one or more of these files contained [ARCHEY's] name, social security number, and direct deposit information (including bank account and routing numbers)[.]" See ECF No. 25, p. 3. Further, OSMOSE admits that it "could not definitively rule out

recognize that the plaintiffs may eventually not be able to provide an adequate factual basis for the inference, but they had no such burden at the pleading stage." *Neiman Marcus*, 794 F. 3d at 694.

the possibility" that ARCHEY's personal information was not "viewed […] accessed, copied, or downloaded […] by the hackers," and accordingly, "offered [ARCHEY] free credit monitoring and identity-theft protection as a precaution." See ECF No. 25, p. 1. Much like in *Neiman Marcus*, OSMOSE offering its employees free credit monitoring and identity-theft protection is an acknowledgment that the risk of future injury from hackers is very real, and thus, is a concrete injury. As the Seventh Circuit in *Neiman Marcus* stated, "stolen data may be held for up to a year or more before being used to commit identity theft." *Neiman Marcus*, 794 F. 3d at 694. Thus, at a minimum at this stage, it is premature to dismiss ARCHEY's claim before he can affirmatively plead some damage other than the data breach.

Further, OSMOSE cites the case of *Moyer v. Michaels Stores, Inc.,* No. 14 C 561, (N.D. Ill. Jul. 14, 2014) for its argument that "conclusory allegations of damages arising from unauthorized access do not suffice to avoid dismissal." See ECF No. 25, p. 6. However, the case of *Moyer* is distinguishable from the case at hand. *Moyer* was a consolidated class action lawsuit involving retail transactions, not employment matters, brought primarily by a plaintiff without standing in the lawsuit because that plaintiff had previously been tangled in a separate action in New York state court against the defendant. *Id.*, at *6-7. In *Moyer*, the Court held that "All of Plaintiffs' alleged injuries [between the New York plaintiff and the others] do not constitute actual economic damage under Illinois law." *See* Moyer, at *18 ("[A]s a matter of law, an increased risk of future harm is an element of damages that can be recovered for a present injury--it is not the injury itself." (citing *Williams v. Manchester*, 888 N.E.2d 1, 13 (Ill. 2008)). Thus, an increased risk of future harm is an element of damages, that combined with more—in this case, ARCHEY's statutory damages related to ARCHEY's PIPA claim (*see infra*) as well as the value of ARCHEY's own time needed to set things straight from an opportunity-cost perspective (*see infra*)—differentiate the present case from *Moyer*. Accordingly,

ARCHEY has sufficiently plead damages and OSMOSE's Motion to Dismiss Count III without leave to amend must be denied.

Likewise, the case of *Worix v. MedAssets, Inc.*, can easily be distinguished from the present case. In *Worix*, another class action lawsuit, the plaintiffs alleged that "an unknown person stole a computer hard drive from a MedAssets employee's car" containing information "including the names, birthdays, and social security numbers of over 82,000 patients, including 32,000 CCHHS patients," and the information "was neither encrypted nor password protected." *Worix v. Medassets, Inc.,* 857 F. Supp. 2d 699, 700 (N.D. Ill. 2012). However, the defendants stated that the hard drive contained "names, encounter numbers and administrative information" but not "addresses, birth date[s], and social security number[s]." *Id.* For the thief in *Worix* to have access to "names, encounter numbers and administrative information" is not the same type of information that would allow a data thief to cause pecuniary harm to his or her victims, unlike here where OSMOSE's cyberattack hackers obtained access to ARCHEY's "name, social security number, and direct deposit information (including bank account and routing numbers)[.]" ECF No. 25, p. 3 (emphasis added).

Finally, the case of *Pisciotta v. Old Nat. Bancorp,* can also easily be distinguished from the present case. In *Pisciotta*, a class action lawsuit, the plaintiffs (made up of a bank's actual and potential customers) alleged that, through its website, the bank had solicited personal information from applicants for banking services but had failed to adequately secure it. *Pisciotta v. Old Nat. Bancorp*, 499 F.3d 629, 631 (7th Cir. 2007). The applications apparently differed depending on the service requested, but some forms required the customer or potential customer's name, address, social security number, driver's license number, birth date, mother's maiden name, and credit card or other financial account numbers. *Id.* As a result, a third-party computer "hacker" was able to obtain access to the confidential information of tens of thousands of bank site users. *Id.*

The district court in *Pisciotta* granted the bank's motion for judgment on the pleadings and denied the plaintiffs' motion for class certification as moot. *Id.*, at 632. Specifically, the district court concluded that the plaintiffs' claims failed as a matter of law because "they have not alleged that [bank's] conduct caused [plaintiffs] cognizable injury." *Id.* In support of its conclusion, the court noted that, under Indiana law, damages must be more than speculative; therefore, the plaintiffs' allegations that they had suffered "substantial potential economic damages" did not state a claim. *Id.* As OSMOSE acknowledges, *Pisciotta* dealt with Indiana law, and not specifically the ICFA. Further, the case was from 2007. Since 2007, the law on this matter has changed. So too have the sophistication of hackers as well as the companies charged with protecting its customers' and employees' data. Companies cannot rely on outdated case law in an attempt to protect themselves instead of its customers and employees.

The case of *Dieffenbach v. Barnes & Noble, Inc.*, from the Seventh Circuit, is also instructional. In *Dieffenbach*, Barnes & Noble discovered in 2012 "that scoundrels had compromised some of the machines, called PIN pads, that it used to verify payment information." *Dieffenbach v. Barnes & Noble, Inc.,* 887 F. 3d 826, 827 (7th Cir. 2018). The hackers acquired details such as customers' names, card numbers and expiration dates, and PINs. *Id.* Some customers temporarily lost the use of their funds while waiting for banks to reverse unauthorized charges to their accounts. *Id.* Some spent money on credit-monitoring services to protect their financial interests. *Id.* Some lost the value of their time devoted to acquiring new account numbers and notifying businesses of these changes. *Id.* Many people use credit or debit cards to pay bills automatically; every time the account number changes, these people must devote some of their time and mental energy to notifying merchants that the old numbers are invalid and new ones must be used. *Id.*

In *Dieffenbach*, the Seventh Circuit, in reviewing case law from the Seventh Circuit and other circuits, noticed that in recent data breach cases, consumers who experienced a theft of their data were

determined to have standing to bring their claims, yet if they did not "adequately plead damages," their claims were dismissed. In response, the Seventh Circuit held the following:

> "This seems to us a new label for an old error. To say that the plaintiffs have standing is to say that they have alleged injury in fact, and if they have suffered an injury then damages are available (if *Barnes & Noble* violated the statutes on which the claims rest). The plaintiffs have standing because the data theft may have led them to pay money for credit-monitoring services, because unauthorized withdrawals from their accounts cause a loss (the time value of money) even when banks later restore the principal, and because the value of one's own time needed to set things straight is a loss from an opportunity-cost perspective. **These injuries can justify money damages, just as they support standing**.
>
> Pleading is governed by Fed. R. Civ. P. 8 and 9. Rule 8(a)(3) requires the plaintiff to identify the remedy sought, but it does not require detail about the nature of the plaintiff's injury. *See Lujan v. Defenders of Wildlife*, 504 U.S. 555, 561, 112 S.Ct. 2130, 119 L.Ed.2d 351 (1992). What's more, Rule 54(c) provides that the prevailing party receives the relief to which it is entitled, whether or not the pleadings have mentioned that relief. Rule 9(g), by contrast, does require details, but only with respect to "special damages." *Barnes & Noble* does not contend, and the district judge did not find, that any loss plaintiffs have identified is treated as "special damages." **As far as the federal rules are concerned, then, all this complaint needed to do was allege generally that plaintiffs have been injured**.
>
> The district court did not apply these rules, instead demanding that the complaint contain all specifics that would have been required had this suit been in state court. 2016 U.S. Dist. LEXIS 137078 at *13-19, 22-25. But in federal court it is the federal rules that determine what must be in a complaint. *See, e.g., Walker v. Armco Steel Corp.,* 446 U.S. 740, 100 S.Ct. 1978, 64 L.Ed.2d 659 (1980); *Gasperini v. Center for Humanities, Inc.,* 518 U.S. 415, 116 S.Ct. 2211, 135 L.Ed.2d 659 (1996); *Shady Grove Orthopedic Associates, P.A. v. Allstate Insurance Co.,* 559 U.S. 393, 130 S.Ct. 1431, 176 L.Ed.2d 311 (2010). **The fact that the federal rules do not require plaintiffs to identify items of loss (except for special damages) means that this complaint cannot be faulted as insufficient.**"

See Dieffenbach, 887 F. 3d at 828 (emphasis added).

Here, pursuant to Fed. R. Civ. P. Rules 8 and 9, and *Dieffenbach*, ARCHEY has sufficiently plead his damages under the ICFA at this time. Accordingly, OSMOSE's Motion to Dismiss Count III, without leave to amend, must be denied.

B. OSMOSE Violated The Illinois Personal Information Protection Act.

OSMOSE argues that ARCHEY cannot establish an ICFA claim based on the Illinois Personal Information Protection Act ("PIPA"). ECF No. 25, p. 10. A violation of IPIPA constitutes an unlawful practice under the ICFA. *See* 815 ILCS 530/20. IPIPA requires data collectors who own personal information concerning an Illinois resident to notify the resident of a data breach "in the most expedient time possible and without unreasonable delay[.]" *See* 815 ILCS 530/10; *see also* argument *supra*.

In re Michaels Stores Pin Pad Litigation, Plaintiffs allege that Michaels violated PIPA by failing to timely notify affected customers of the nature and extent of the security breach. *In re Michaels Stores Pin Pad Litigation,* 830 F. Supp. 2dat 527-28. Michaels responded that it timely notified consumers of the security breach and properly provided consumers with substitute notice. *Id.* The Court, however, held that "a disputed issue of facts exist[ed] regarding when Michaels first learned of the data breach and, thus, whether Michaels timely notified consumers[,]" therefore, "Michaels cannot overcome this disputed issue by relying on self-serving statements from its website that it learned of the security breach the same week it notified consumers." *Id.* Accordingly, the Court held, "Plaintiffs state[d] a plausible claim under the ICFA based on Michaels' alleged violation of PIPA." *Id.*

Here, OSMOSE suffered a cyberattack on July 13, 2020 and did not send ARCHEY notice of the attack until it mailed him its Notice letter on September 2, 2020. *See* Am. Compl., ¶¶ 30-32. Archey did not receive this letter until after he had already filed his original Complaint on September 4, 2020. In his Amended Complaint, ARCHEY alleges that OSMOSE failed to safeguard its' employees' personal information, and subsequently failed to timely notify ARCHEY that such personal information had been compromised, in violation of the PIPA. *See* Am. Compl., ¶¶ 45-48. Regardless of whether OSMOSE subjectively believes it gave timely notice of the cyberattack to ARCHEY, there is a genuine issue of material fact regarding whether OSMOSE gave timely notice of the cyberattack,

an issue which cannot be determined at this time without more information. Accordingly, OSMOSE's Motion to Dismiss Count III must be denied.

CONCLUSION

For the reasons set forth above, Defendant OSMOSE's Motion to Dismiss Counts II and III of Plaintiff ARCHEY's Amended Complaint without leave to amend, must be denied. However, in the event the Motion is granted, Plaintiff respectfully requests that this Court grant Plaintiff the ability to request leave to amend.

Respectfully submitted,
BENNIE ARCHEY

/s/ Matthew R. Custardo
One of his attorneys

Cynthia N. Pietrucha (ARDC #: 6315653)
PIETRUCHA LAW FIRM, LLC
1717 N. Naper Blvd., Suite 200
Naperville, Illinois 60563
Tel.: 630-344-6370
cpietrucha@pietruchalaw.com

Matthew R. Custardo (ARDC #: 06329579)
CUSTARDO LAW, LLC
300 S Carlton Avenue, Suite 210
Wheaton, IL 60189
Tel: 630-557-1451 | Fax: 630-557-8050
matt@custardolaw.com

CERTIFICATE SERVICE

The undersigned attorney hereby certifies that on January 21, 2021, I electronically filed the foregoing **Plaintiff's Response to Defendant's Motion to Dismiss** with the Clerk of the United States District Court for the Northern District of Illinois, Eastern Division, Chicago, Illinois, by using the CM/ECF system, which will send notification of such filing to all CM/ECF participants in this matter, as shown below:

Justin R. Donoho (ARDC #6299667)
BAKER & HOSTETLER LLP
One North Wacker Drive, Suite 4500
Chicago, Illinois 60606-2841
jdonoho@bakerlaw.com

Christopher A. Wiech
BAKER & HOSTETLER LLP
1170 Peachtree Street, Suite 2400
Atlanta, Georgia 30309-7676
cwiech@bakerlaw.com

Joel W. Rice
James M. Hux, Jr.
FISHER & PHILLIPS LLP
10 S. Wacker Drive
Suite 3450
Chicago, IL 60606
jrice@fisherphillips.com
jhux@fisherphillips.com

and I certify that I have mailed same via the United States Postal Service to the following non-CM/ECF participants:

None.

/s/ Matthew R. Custardo

Cynthia N. Pietrucha (ARDC #: 6315653)
PIETRUCHA LAW FIRM, LLC
1717 N. Naper Blvd., Suite 200
Naperville, Illinois 60563
Tel.: 630-344-6370
cpietrucha@pietruchalaw.com

Matthew R. Custardo (ARDC #: 06329579)
CUSTARDO LAW, LLC
300 S Carlton Avenue, Suite 210
Wheaton, IL 60189
Tel: 630-557-1451 | Fax: 630-557-8050
matt@custardolaw.com